IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Shiwen Chen	:	
Serial No.:	10/614,542	:	Group: 2152
Filed:	August 7, 2003	:	Examiner: Angela Widhalm
For:	TRAVERSABLE NETWORK ADDRESS TRANSLATION (TNAT) WITH HIERARCHICAL INTERNET ADDRESSING ARCHITECTURE	:	

AFFIDAVIT UNDER 37 C.F.R.1.132

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Shiwen Chen declares as follows based on his personal knowledge:

that he is the inventor who on August 7, 2003 filed the above identified application;

that he is an expert in the field of information networks employing NAT routers;

that he has reviewed and understood the teachings of Park (U.S. Pub. No. 2003/0031173), Martin et al. (U.S. Pat. App. Pub. No. 2004/0073640), and Farinacci et al. (U.S. Pat. No. 7,016,351);

that Farinacci et al. do not teach, suggest, or motivate two or more private addresses appended to one another in a predefined order and defining a path to a device in a private network;

that Faranacci et al. merely teach using a proprietary protocol to discover a multicast path and set up a source address routing list, which cannot be applied to networks with NAT routers, since a tracing packet for the purpose of route setup cannot traverse the entire network to get a source routing list;

that Farinacci et al. is in a different field of endeavor because the differences in structure and function reveal that the teachings of Farinacci et al. are not relevant to the particular problem with which the inventor is involved;

that Farinacci et al. is not reasonably pertinent to the problem with which the inventor was concerned because a person having ordinary skill in the art would not reasonably have expected to solve the problem of destination routing in private networks by considering a reference dealing with source routing using a list of public addresses;

that Park (U.S. Pub. No. 2003/0031173) in view of Martin et al. (U.S. Pat. App. Pub. No. 2004/0073640) and Farinacci et al. (U.S. Pat. No. 7,016,351), for reasons detailed below, do not teach suggest or motivate a Nat router that: receives a data packet having a packet header including a destination IP address field, a source IP address field, and an options field having a stack of two or more private IP addresses appended to each other in a predefined order and defining a path to a source device in a private network; extracts a private IP address directly from the options field; directly formats_the destination IP address field of the packet header with the extracted private IP address prior to forwarding the data packet; and reformats the options field to remove the extracted private IP address from the stack prior to forwarding the data packet:

> Network Address Translation is largely deployed in the Internet as a solution to the problem of insufficient IPv4 address. However NAT routers divide the Internet into one shared public network and countless private network "islands".

Although NAT allows one "private" device to be able to initiate communications with a public device, and allows limited servers in a private network APPEAR to be public devices with fixed address/port mapping, it is still difficult for an arbitrarily located device (i.e. either a public device or a device in a private network X) to initiate a communication session with a private device (in private network Y). This is inherently difficult because a NAT router does not really solve the insufficient address space problem, and must use a limited pool of numbers(a NAT router's IP address + a set of TCP/UDP port numbers) to support the mapping of private devices, this has to be dynamic because almost all private devices have to share this limited pool. The dynamic mapping therefore has to be established by an insider (a device within the NAT router's private network). Before a dynamic mapping exists, an outsider (a device within public network or another private network) is not able to reach the insider as the insider's public APPEARANCE (the mapping to the pubic address/port) is unknown. In other words, a public appearance of a private network device does not exist before the insider private network device initiates a communication session; therefore, when a outsider attempts to establish a session to an insider, even if it uses source routing scheme, it cannot find a proper mapping (public appearance) of the insider. Therefore the source routing will fail. This brings problems to peer-to-peer communications (such as voice over IP) which requires addresses of both ends are unique and exist before a communication starts.

Therefore, the invention in this application breaks the NAT-divided public-private barrier by establishing a new addressing architecture without major changes to the Internet protocol (IPv6 is a siginificant change to the current Internet). By allowing private addresses cascaded to a public address, any device (as long it is connected to the Internet) is uniquely identifiable on the Internet so that any other devices may use the unique cascaded address to reach the device. By allowing embedding those private addresses in a IPv4 packet, the invention solution is compatible to the current Internet and NAT technology, and allows smooth transition to the new addressing architecture.

Furthermore, the cascading address architecture allows nested private networks, and the private addresses are possible to be non-IP addresses, which brings possibility of integrating more non-IP private networks.

So in summary, here are the major functional features and/or advantages in this invention application:

a cascading addressing scheme implemented by NAT routers that uniquely identifies a device located in possibly nested private networks;

a method performed at NAT routers that incorporates the new cascading addressing scheme into the existing IPv4-based Internet routing method to enable true peer-to-peer communications between any devices:

devices can be anywhere: public, private, or nested private networks,

devices anywhere can initiate communication sessions to devices anywhere,

new NAT routers that implement this new method can still be compatible to existing Internet and existing NAT technologies, enabling seamless migration of Internet evolution;

new NAT routers that implement this new method can extend the support to non-IP networks and devices;

new NAT routers that implement this new method accomplish elimination of the concept/barriers of public vs. private networks when this new scheme and method is deployed;

new NAT routers that implement this new method ensure that, even when a NAT establishes a mapping between an insider private address and its public appearance (i.e., the public address and a TCP/UDP port number), this mapping is "session-based": only the device in the same communication session is able to see the insider's public appearance; any other outsider devices still are NOT able to reach this insider device, even though it is communicating with someone.

that all statements made herein of their own knowledge are true and that all statements made on information and belief are believed to be true; and

that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under

Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Shiwen Chen

12/11/2007

Date